EXHIBIT 1

17 MAG 6961

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of an Application for Search Warrants for Stored Electronic Communications

SEALED
AGENT AFFIDAVIT

_____ Mag. _____

Application for Search Warrants for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

JEFF D. DONALDSON, being duly sworn, deposes and states:

I. Introduction

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified

information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

II. The Target Accounts

3. I make this affidavit in support of an application for search warrants pursuant to 18 U.S.C. § 2703 directed to Google, Inc., headquartered in Mountain View, CA ("Google"); Reddit, Inc., headquartered in San Francisco, CA ("Reddit"), and Github.com, headquartered in Sacramento, CA ("GitHub"), (collectively, "Providers"), for all content and other information associated with the following "**Target Accounts**":

a. The Google account associated with the email address joshschulte1@gmail.com (the "**Subject Google Account**"), which is maintained and controlled by Google.

b. The Reddit account associated with the account name L1347517 (the "**Subject Reddit Account**"), which is maintained and controlled by Reddit.

c. The GitHub account associated with the user name pedbsktbll (the "**Subject GitHub Account**"), which is maintained and controlled by GitHub.

4. The information to be searched is described in the following paragraphs and in Attachment A to each of the proposed warrants.

Google

5. Based on my training, experience, and participation in this investigation, I know the following about Google:

a. Google offers email and other Internet-based services to the public. Among other things, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using Google's services can access his or her email account from any computer connected to the Internet, and can link any variety of Google's other Internet-based services to his/her Gmail account.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents*. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers

indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vi. *Preserved records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

c. In addition, subscriber information for the Subject Google Account indicates that the subscriber of the Subject Google Account has activated additional online Google Services, and, accordingly, the Provider also maintains, among other things, the following records and information with respect to the **Subject Google Account**:

i. *Google Drive.* Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through the service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

ii. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive. Users can also download such documents in various formats, such as a Microsoft Word document (e.g., ".docx"), an OpenDocument Format (".odt"), Rich Text Format (".rtf"), a PDF document (".pdf"), or Plain Text document (".txt").

iii. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means

of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

iv. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

v. *YouTube content.* Google allows subscribers to maintain linked YouTube accounts, a global video-sharing website that allows users to upload and share videos with public on the Internet. Registered users can upload an unlimited number of videos and add comments to videos.

vi. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's email and chat content.

vii. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location.

Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

viii. *Android Services.* Google also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by Google, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (the International Mobile Station Equipment Identifier), MEID (the Mobile Equipment Identifier), device ID, and/or serial number of the devices. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

ix. *Google Voice.* Google provides a telephone service that provides call forwarding and voicemail services, voice and text messaging.

x. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

xi. *Web History.* Google maintains searches and account browsing activity, from Chrome, Google's proprietary web browser, as well as other Google applications.

Reddit

6. Based on my training, experience, and participation in this investigation, I know the following about Reddit:

a. Reddit operates several products and services, including reddit.com, redditgifts.com, and associated Reddit mobile applications. The most popular product is reddit.com, which provides an online forum where people can create communities (known as "subreddits") in which users can communicate online.

b. Each subreddit on reddit.com has its own page, subject matter, users, and moderators. Users post stories, links, and media to these communities, and other users can comment and can "upvote" or "downvote" a post.

c. The information that is collected by Reddit varies depending on what services the user utilizes. For example, if the user signs up to post on the website reddit.com, Reddit users can choose to provide their name and other contact information (including, but not limited to, their email address), although though users can also choose not to do so. If the user signs up to Reddit Gifts, the user may be asked to provide Reddit with personal information such name, address, telephone number, age, personal interests, and email address. The user may also be required to provide log-in information for an existing Reddit Account or to create one before using Reddit Gifts.

GitHub

7. Based on my training, experience, and participation in this investigation, I know the following about GitHub:

8. Based on my training, experience, and participation in this investigation, I know the following about GitHub:

a. GitHub is a web-based Git, or version control repository, and Internet-hosting service, that can be accessed at https://github.com/. GitHub allows Internet users to host code, manage projects, and build software alongside millions of other developers.

[redacted]

b. A user must create an account in order to contribute content to the site, but public repositories can be browsed and downloaded by others. When an individual registers for an account, they are able to discuss, manage, create repositories, submit contributions to others' repositories, and/or review changes to code. Users are represented in GitHub's system as personal GitHub accounts. Each user has a personal profile, and can own multiple repositories. Users can create or be invited to join organizations, or to collaborate on another user's repository. A repository is one of the most basic GitHub elements. It can contain project files (including documentation), and stores each file's revision history.

c. A variety of information is available on GitHub about users and their repositories. Public user profiles can include username, repositories that the user has starred, other GitHub users the user follows, and those that follow the user. A user may also choose to not share his or her real name, avatar, affiliated company, location, public email address, personal web page, or organizations to which the user belongs.

d. GitHub provides social networking-like functions such as feeds, followers, wikis (using wiki software called Gollum) and a social network graph to display how developers work on their versions of a repository and what version is newest.

e. GitHub can be accessed on GitHub.com, or through GitHub Enterprise on one's own server, or in a private cloud using Amazon Web Services. GitHub Enterprise is similar to GitHub's public service, but is designed for use by large-scale enterprise software development teams where the enterprise wishes to host their repositories behind a corporate firewall.

III. Jurisdiction to Issue the Requested Warrants

9. Pursuant to Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, Reddit, or GitHub, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

10. A search warrant under Section 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

11. When the Government obtains records under Section 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

IV. The Subject Offenses

12. For the reasons detailed below, I believe that there is probable cause to believe that the Target Accounts contain evidence, fruits, and instrumentalities of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the

United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses").

V. Probable Cause

A. WikiLeaks Publication of Classified CIA Information

13. Based on my review of publicly available material on the Internet, including on the website wikileaks.org ("WikiLeaks"), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the "Classified Information") belonging to the Central Intelligence Agency ("CIA"). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was "the largest ever" unauthorized publication of classified CIA documents.

b. The Classified Information constituted the "first full part" of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.

c. The "collection" obtained by WikiLeaks amounted to "more than several hundred million lines of code" and revealed the "entire hacking capacity" of the CIA, including various malware, viruses, and other tools used by the CIA.

14. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact,

[redacted] 2017-03-14

classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the "CIA Group"). That CIA Group exists within a larger CIA component (the "CIA Component"). In March 2016, less than 200 employees were assigned to the CIA Group. And only employees of the CIA Group had access to the computer network on which the Classified Information that was stolen from the CIA Group's computer network was stored. (Moreover, as described in detail below, only three of those approximately 200 people who worked for the CIA Group had access to the specific portion of the Group's computer network on which the Classified Information was likely stored.)

c. The Classified Information appears to have been stolen from the CIA Component sometime between the night of March 7, 2016 and the night of March 8, 2016.

i. This is based on preliminary analysis of the timestamps associated with the Classified Information which indicates that March 7, 2016 was the latest (or most recent) creation or modification date associated with the Classified Information.

ii. Because, for the reasons described below (*see infra*), the Classified Information was apparently copied from an automated daily back-up file, it is likely that the Classified Information was copied either late on March 7, 2016 (after the March 7 nightly back-up was completed) or on March 8, 2016 (before the March 8 nightly back-up was completed).

iii. This is so because if the Classified Information was copied before the March 7 back-up, one would *not* expect to see in the Classified Information documents dated as late as March 7. And if the Classified Information was copied after the March 8 back-up, one *would* expect to see documents dated on or after March 8 because the "back-ups" occur

approximately each day.[1]

d. The Classified Information was publicly released by WikiLeaks exactly one year to the day (March 7, 2017) from the latest date associated with the Classified Information (March 7, 2016).

e. The duplication and removal from the CIA Group's computer network of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury to the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

B. The CIA Group's Local Area Computer Network (LAN) and Back-Up Server

15. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the Classified Information originated

[1] It is of course possible that the Classified Information was copied later than March 8, 2016 even though the creation/modification dates associated with it appear to end on March 7, 2016. For example, the individual who copied and removed the data could have limited his or her copying to data that was modified or created on or before March 7, 2016. (Conversely, however, the Classified Information is unlikely to have been copied before March 7, 2016, because it contains data that was created as recently as March 7, 2016.) Because the most recent timestamp on the Classified Information reflects a date of March 7, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 7 and the end of the day on March 8.

in a specific isolated local area computer network ("LAN") used exclusively by the CIA Group.[2] As described above, in and around March 2016, in total less than 200 people had access to the CIA Group's LAN on which the Classified Information was stored.

a. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

b. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

c. The CIA Group's LAN, and each of its component parts, was maintained in heavily physically secured governmental facilities, which include multiple access controls and various other security measures.

d. The isolated LAN used by the CIA Group was comprised of multiple networked computers and servers. (Each of these component computers and servers were, by definition, inside the electronically isolated LAN.)

i. In order to preserve and protect the CIA Group employees' day-to-day computer engineering work, that work was backed up, on an approximately daily basis, to another server on the CIA Group's LAN that was used to store back-up data (the "Back-Up Server").

ii. Back-ups of the sort stored on the Back-Up Server are designed to ensure that, should the original data be corrupted or deleted, the stored data is not lost, but rather—because of the daily back-ups—is maintained via the daily copies stored on the Back-Up

[2] In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from "an isolated, high-security network."

Server.

C. The Publicly Disclosed Classified Information Likely Originated on the CIA Group's Back-Up Server

16. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I understand that the Classified Information that was publicly released by WikiLeaks appears likely to have been copied—specifically—from the CIA Group's Back-Up Server.

a. As described above, the Back-Up Server served as a secondary storage location for data that principally resided on the primary computer network used for CIA Group employees' day-to-day work writing computer code. Approximately each day, an automated process would back-up that data to the Back-Up Server. Each of those daily back-ups was akin to an electronic "snapshot" of the data on that particular date. In that way, the Back-Up Server simultaneously acquired and stored, on a rolling basis, daily snapshots of the original data.

b. As such, if the data contained on the Back-Up Server was copied *en masse* directly from that Server, the copy would contain numerous iterations (or snapshots) of the similar or same data which had been backed up from the original data, distinguished by date.

c. The publicly released Classified Information does in fact contain numerous iterations (or snapshots) of the similar or same data, distinguished by date.

d. Accordingly, the fact that the Classified Information contains numerous iterations (or snapshots) of the similar or same data, distinguished by date, is strongly supportive of the fact that the Classified Information was taken from the CIA Group's Back-Up Server.[3]

[3] I understand, based on my conversations with others familiar with the CIA Group's LAN that it would be difficult, if not impossible, to copy from the data (not on the Back-Up Server) the multiple different date-distinguished iterations of the same data that are included in the publicly released Classified Information. In contrast, a single copy of the Back-Up Server

e. As described above, because the most recent timestamp associated with the Classified Information appears to be March 7, 2016, it is likely that the Classified Information was copied from the Back-Up Server after the daily back-up on March 7, 2016, and before the daily back-up on March 8, 2016.

D. TARGET SUBJECT JOSHUA ADAM SCHULTE Was One of Only Three Employees Across the Entire CIA Who, in March 2016, Had Been Given System Administrator Access to the Back-Up Server

17. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the CIA Group's LAN was designed such that only those employees who were specifically given a particular type of systems-administrator access ("Systems Administrators") could access the Back-Up Server.

a. Systems Administrators were given a particular username and password in order to log on to and access the Back-Up Server.

b. Conversely, CIA employees who were not designated Systems Administrators were not given access to the Back-Up Server.[4]

18. I know, based on my conversations with other law enforcement agents and others, in approximately March 2016—the month when the Classified Information is assessed to have been copied—only three CIA employees were designated Systems Administrators with access to the CIA Group's Back-Up Server.

---

would likely include each of the prior iterations (or snapshots) of the same data—which is exactly what is reflected in the publicly released Classified Information.

[4] It is, of course, possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated Systems Administrator. Or an employee lacking Systems Administrator access could, at least theoretically, gain access to the Back-Up Server by finding a "back- door" into the Back-Up Server.

a. TARGET SUBJECT JOSHUA ADAM SCHULTE ("SCHULTE") was one of those three Systems Administrators.

i. SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA.

ii. During SCHULTE's more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information.

iii. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As described above, in March 2016, SCHULTE was one of only three CIA employees throughout the entire CIA who had authorized access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. The publicly released Classified Information published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia,* multiple CIA employees—including two of the three aforementioned individuals with designated Systems Administrator privileges.

i. Names used by the other two CIA Group Systems Administrators were, in fact, published in the publicly released Classified Information.

ii. SCHULTE' s name, on the other hand, was not apparently published in the Classified Information.

iii. Thus, SCHULTE was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks's publication of the Classified Information.

c. The other two individuals who served in March 2016 as Systems Administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

E. SCHULTE Had Access to the Back-Up Server on March 7 and 8, 2016—The Likely Dates of the Copying of the Classified Information

19. As described above, it appears likely that the Classified Information was copied between March 7 and March 8, 2016.

a. Based on my conversations with other law enforcement agents and others, and my review of documents, including access records of the CIA Component facility in which SCHULTE worked, I know that he was present at work from approximately:

i. 10:01 a.m. until 7:16 p.m. on March 7, 2016; and

ii. 10:19 a.m. until 7:40 p.m. on March 8, 2016.

b. Based on my conversations with other law enforcement agents and others, and my review of documents, I know that on March 8, 2016, the CIA Group held an offsite management retreat for many of its senior and midlevel managers. Accordingly, on March 8th, much of the CIA Group's management, including some to whom SCHULTE reported, were not present in the CIA Component building where SCHULTE and other CIA Group employees worked.

c. I further understand that SCHULTE's workspace (*i.e.*, his desk and computer workstation) was set up such that only three other CIA Group Employees had direct line-of-sight to SCHULTE's desk and computer—that is, only three other employees could see what he was doing at his desk. At least two of those three employees were at the offsite management retreat on March 8, 2016.

d. As described above, in March 2016, only two CIA employees in addition

to SCHULTE were designated Systems Administrators with access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. On March 8, 2016, one of those two other designated Systems Administrators was at the offsite management retreat. (The retreat was held at a location that did not have any access to the CIA Group's LAN, including the Back-up Server, and therefore afforded no access to the Classified Information.)[5]

F. SCHULTE's Unauthorized Unilateral Reinstatement of His Own Administrative Privileges

20. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, on or about April 4, 2016, around the time of his reassignment to another branch within the CIA Group, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a Systems Administrator in the CIA Group's LAN.

a. At the same time, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1.

b. Upon that transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.[6]

c. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and

[5] On March 7 and 8, 2016, the third of the three CIA employees with Systems Administrator access was located at a CIA facility that did, in fact, have access to the Back-Up Server from which the Classified Information was likely copied.

[6] SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

21. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, less than two weeks later, on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

a. On or about April 14, 2016, CIA Group management discovered that SCHULTE had personally re-instituted his administrator privileges without permission.

b. On or about April 18, 2016, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. SCHULTE signed an acknowledgment that he understood that "individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system." That notice further instructed SCHULTE: "do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed."

c. A little more than one month later, on May 26, 2016, and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1. Before receiving a response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

i. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

ii. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, "You were aware of the policy for access and your management's lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges." It continued by warning SCHULTE that any future violations would result in "further administrative action of a more severe nature."

iii. After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

22. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that SCHULTE's accessing of information on the LAN that he had been expressly forbidden by the CIA to access, and his accessing of information which he had been electronically prevented from accessing by the CIA, using a computer network on which he was permitted to access other, distinct information, exceeded his authorized access to the government-owned and controlled computer networks of the CIA. *See* 18 U.S.C. § 1030(a)(1) & (a)(2)(B).

G. Internal CIA Investigation of SCHULTE and a CIA Colleague

23. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in or around March 2016, SCHULTE came to the attention of CIA security after SCHULTE alleged that another CIA Group co-worker had made a threat against him. SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat. He threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident. SCHULTE informed CIA security that, if "forced into a corner" he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media. In addition, CIA security learned that

SCHULTE had removed an internal CIA document from CIA facilities that regarded his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so.

24. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

a. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

b. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

c. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.[7]

H. SCHULTE's November 2016 Resignation from the CIA

25. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in connection with and preceding SCHULTE's November 2016 resignation from the CIA, he sent the following communications,

[7] External drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

among others:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *EYES ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "veiled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved."

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, "ignored" issues he had raised about "security concerns" and had attempted to "conceal these practices from senior leadership," including that the CIA Group's LAN was "incredibly vulnerable" to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and "later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing]

environment entirely on me."[8]

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had "left [the CIA Group's LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet."

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that office that he had been in contact with the United States House of Representatives' Permanent Select Committee on Intelligence regarding his complaints about the CIA ("OIG Email").

i. In the OIG Email, which SCHULTE labeled "Unclassified," SCHULTE raised many of the same complaints included in the draft "Letter of Resignation 10/12/16," described above, including the CIA's treatment of him and its failure to address the "security concerns" he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE's colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked.

iii. Notwithstanding SCHULTE's labeling of the email as "Unclassified," the CIA subsequently determined that the OIG Email which SCHULTE removed from the CIA without authorization did, in fact, contain classified information.

---

[8] SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues (*see supra* at Part II.G.16).

I. SCHULTE' s Use Of the Subject Google Account To Make Inquiries About the Status of the Investigation

26. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, since the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE has repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues have reported that contact to government and law enforcement officials.

a. In those communications with his former colleagues, SCHULTE has repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. SCHULTE has requested more details on the information that was disclosed.

c. SCHULTE has inquired of his interlocutors' personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE has also asked what other former CIA Group colleagues are saying about the disclosure.

d. SCHULTE has repeatedly denied any involvement in the disclosure of the Classified Information.

e. SCHULTE has indicated the he believes that he is a suspect in the investigation of the leak of Classified Information.

f. I am not aware of any other former CIA employee who has initiated any contact with former colleagues regarding the disclosure of the Classified Information.

27. Furthermore, I know that SCHULTE has specifically used the **Subject Google Account**, *i.e.*, the account associated with the Gmail account joshshulte1@gmail.com, to make

some of the inquiries described above. For example:

a. Records show that, on or about March 7, 2017, when WikiLeaks released the Classified Information, SCHULTE used the Google Voice feature associated with the **Subject Google Account** to send approximately 149 texts to multiple of his former colleagues at the CIA.

b. SCHULTE, using the Google Voice feature associated with the **Subject Google Account**, also had phone calls with former CIA colleagues, including one telephone call with a former colleague in which he, among other things, inquired of the former colleague's personal opinions regarding who was responsible for the disclosure of the Classified Information and what the person's motivation might be. SCHULTE indicated that he believed that the person responsible was a contractor who disclosed the Classified Information for fame.

c. In a call using the telephone number associated with the Subject Google Account on March 8, 2017 with the same former colleague, SCHULTE denied his involvement in the disclosure of the Classified Information, indicated his belief that many people suspected him of the disclosure, and relayed a conversation with another acquaintance in which SCHULTE had denied involvement in the disclosure of the Classified Information, but was dissatisfied with the acquaintance's reaction to SCHULTE's denial.

d. Records for recent communications on the Gmail feature of the Subject Google Account show that SCHULTE also continues to use various Google Services to communicate with others, including his Gmail address joshschulte1@gmail.com, which is listed as the recipient facility for several messages SCHULTE has received in the past two days. As discussed above, SCHULTE's account also reflects as recently as this month his enrollment in other Google Services, including Android, Google Docs, Google Drive, Google Groups, Google

Calendar, Google Hangouts, Google Payments, Google Photos, Google+, and Google Code.

J. The Subject Reddit Account and the Subject GitHub Account

28. Based on my conversations with other law enforcement agents and others, and my review of documents, I also know that references to SCHULTE in the context of the release of the Classified Information have been made on other websites, including those hosted by Reddit and GitHub. Specifically:

a. On or about March 7, 2017—i.e., the date of the release of the Classified Information by WikiLeaks—a "thread," or online discussion, was opened by a Reddit user which was devoted to the release of the Classified Information.

b. As part of the thread, the user of the **Subject Reddit Account** made a post that stated: "What about this guy pedbsktbll?" (with the word "pedbsktbll" highlighted). The comment was followed by, among other things, (1) a listing of the following website: https://github.com/pedbsktbll/projectwizard/blob/master/ProjectWizard/tempSubmodule.xml (the "Website") and (2) a line of text stating, "pedbsktbll -> Joshua Schulte."

c. I know, based on a review of publicly available websites, including those available through various social media sites, that SCHULTE employs the user name "pedbsktbll" on various of these websites. For example, I know from reviewing a posting on the Google+ service associated with the Subject Google Account, which contains a photograph of SCHULTE, that SCHULTE listed various of his other social media accounts, several of which (e.g., including Facebook and Twitter) contain or reference the user name "pedbsktbll."

29. I also know from viewing the Website, which features a page associated with the **Subject GitHub Account**, that the Webpage contains numerous lines of computer code, some of which reference computer applications that were referenced in the information released by WikiLeaks.

30. I respectfully submit that there is probable cause therefore to believe that the Target Accounts contain evidence, fruits, and instrumentalities of the Subject Offenses. Among other things, I respectfully submit that there is probable cause to establish that SCHULTE is proficient in and makes use of Internet-based computing services, like those offered by the Providers through the Target Accounts. Moreover, based on my training and experience, I know that individuals who engage in the Subject Offenses often use Internet-based services (like the Target Accounts) as a means by which to communicate with co-conspirators as well as means through which not only to transmit but also to store purloined information so that they do not have to carry it on their person. Finally, I know that individuals who engage in the Subject Offenses oftentimes use Internet-based computing services, like the Target Accounts, to publish purloined information. For example, based on my training and experience and my involvement in this investigation, I know that WikiLeaks is an Internet-based publication and that individuals who provide information to WikiLeaks in the past oftentimes have done so through the use of other Internet-based computing platforms, like the Target Accounts and other services offered by the Providers. Accordingly, when each of these factors is considered in conjunction with the fact of SHCULTE's access to the purloined information, his clear proficiency in computers and computer-programming, and the probable cause establishing SCHULTE's access to and use of the Subject Accounts, I respectfully submit that there is probably cause to believe that the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses.

K. SCHULTE' s Planned Travel

31. Based on my conversations with other law enforcement agents and others, and my review of documents, including information provided by the Department of Homeland Security, I understand that SCHULTE has booked an international flight departing on Thursday, March 16, 2017. (Return travel to the United States is booked for a few days later.) The

aforementioned records and conversations reflect that this is only SCHULTE's second trip reflected in in DHS records outside the United States.

VI. Evidence, Fruits and Instrumentalities in Target Accounts

32. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the **Target Accounts** will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the requested warrants.

33. In particular, I believe the **Target Accounts** are likely to contain, among other things, the following information:

a. Evidence of the identity(s) of the user(s) of the **Target Accounts** as well as other coconspirators in contact with the **Target Accounts**;

b. Evidence relating to the participation in the Subject Offenses by the users of the **Target Accounts** and others, including information relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

c. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

d. Items, records or information consisting of, referring to, or reflecting classified documents or materials on the **Target Accounts**;

e. Evidence concerning financial institutions and transactions used by the users of the **Target Accounts** in furtherance of the Subject Offenses;

f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the **Target Accounts**;

g. Passwords or other information needed to access any such computers, accounts, or facilities; and

h. With respect to the Subject Google Account, evidence relating to the geolocation and travel of the user(s) of the **Target Accounts** at times relevant to the Subject Offenses.

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which will be directed to produce a digital copy of any responsive records to law enforcement personnel within 10 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the requested warrants, which shall not be transmitted to the Providers.

35. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all content associated with the **Target Accounts**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine

which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, to the extent applicable, including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

VII. Request for Non-Disclosure and Sealing Orders

36. The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrants could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

37. Accordingly, there is reason to believe that, were the Providers to notify the subscriber(s) or others of the existence of the requested warrants, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the

Court direct the Providers not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

38. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter

Special Agent Jeff D. Donaldson
Federal Bureau of Investigation

Sworn to before me this
14th day of March, 2017

HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

2017-03-14

JAS_000125

17 MAG 6961

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information for the Google account associated with Email Address joshschulte1@gmail.com, Maintained at Premises Controlled by Google, Inc. and Google Payment Corp.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. and Google Payment Corp. ("Google")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Google associated with the email address joshschulte1@gmail.com contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Google is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Google within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Google is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Google shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Google may disclose this Warrant and Order to an attorney for Google for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Google; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 — Date Issued

1:11 AM — Time Issued

THE HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to Google, Inc. and Google Payment Corp. (collectively, "Google" or the "Provider") and applies to all content and other information within Google's possession, custody, or control that is associated with the email address joshschulte1@gmail.com (the "Subject Gmail Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Google

To the extent it is within Google's possession, custody, or control, Google is directed to produce the following information associated with the Subject Gmail Account:

a. Search History. All data concerning searches run by the user of the Subject Gmail Accounts, including, but not limited to, the content, date, and time of the search.

b. Google+ Photos and Content. All data concerning Google+ Photos, including all albums, photos, videos, and associated metadata for each file, as well as all Google+ posts, comments, profiles, contacts, and information relating to Google+ Circles.

c. Google Drive Content. All files and folders in the Google Drive associated with the Subject Gmail Account.

d. Google Voice. All records, voicemails, text messages, and other data associated with Google Voice.

e.

f. Google Wallet Content. All data and information in the Google Wallet associated with the Subject Gmail Account.

g. YouTube Content. For any YouTube account associated with the Subject Gmail Account, all subscriber information as well as copies of any videos and associated metadata and any YouTube comments or private messages.

h. Android Content. Any Android device information associated with the Subject Gmail Account, including IMEI/MEID, make and model, serial number, date and IP of last access to Google, and a list of all accounts that have ever been active on the device.

i. Email Content. All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Gmail Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

j. Address book information. All address book, contact list, or similar information associated with the Subject Gmail Account.

k. Subscriber and payment information. All subscriber and payment information regarding the Subject Gmail Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

l. Linked accounts. The account identifiers for all accounts linked to the Subject Gmail Accounts, and subscriber records therefore as described in the preceding sub-paragraph,

including but not limited to any account linked to the Subject Gmail Account by registration IP address, "machine" or other cookie, alternate email address, or telephone number.

m. Transactional records. All transactional records associated with the Subject Gmail Account, including any IP logs or other records of session times and durations.

n. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Gmail Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

o. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Google in order to locate any evidence, fruits, and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States,

in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses"), including the following:

i. Evidence of the identity(s) of the user(s) of the Subject Gmail Account as well as other coconspirators in contact with the Subject Gmail Account;

j. Evidence relating to the geolocation and travel of the user(s) of the Subject Gmail Account at times relevant to the Subject Offenses;

k. Evidence relating to the participation in the Subject Offenses by the users of the Subject Gmail Account and others;

l. Evidence concerning financial institutions and transactions used by the users of the Subject Gmail Account in furtherance of the Subject Offenses;

m. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

n. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Gmail Account; and

o. Passwords or other information needed to access any such computers, accounts, or facilities.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

17 MAG 6961

In the Matter of a Warrant for All Content and Other Information for the Reddit, Inc. account associated with account name L1347517, Maintained at Premises Controlled by Reddit, Inc.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Reddit, Inc.

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Reddit, Inc. associated with account name L1347517 contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Reddit, Inc. is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Reddit, Inc. within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Reddit, Inc. is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Reddit, Inc. shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Reddit, Inc. may disclose this Warrant and Order to an attorney for Reddit, Inc. for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Reddit, Inc.; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 — Date Issued

1:12 AM — Time Issued

THE HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to Reddit, Inc. (the "Provider") and applies to all content and other information within Reddit, Inc.'s possession, custody, or control that is associated with the account name L1347517 (the "Subject Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Reddit, Inc. Reddit, Inc. is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Reddit, Inc.

To the extent it is within Reddit, Inc.'s possession, custody, or control, Reddit, Inc. is directed to produce the following information associated with the Subject Account:

a. Search History. All data concerning searches run, and posts accessed by the user of the Subject Account, including, but not limited to, the content, date, and time of the search or post access.

b. Post Content. All posts and messages made by the Subject Account, including all content, attachments, and any other information (specifically including the date and time at which each post or message was made/sent, and the size and length of each post/message).

c. Email Content or Direct Message Content. All emails and/or direct messages sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and

destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

d. Subscriber and payment information. All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

e. Transactional records. All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

f. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

g. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Reddit, Inc. in order to locate any evidence, fruits, and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to

believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses"), including the following:

p. Evidence of the identity(s) of the user(s) of the Subject Account as well as other coconspirators in contact with the Subject Account;

q. Evidence relating to the geolocation and travel of the user(s) of the Subject Account at times relevant to the Subject Offenses;

r. Evidence relating to the participation in the Subject Offenses by the users of the Subject Account and others;

s. Evidence concerning financial institutions and transactions used by the users of the Subject Account in furtherance of the Subject Offenses;

t. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

u. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Account; and

v. Passwords or other information needed to access any such computers, accounts, or facilities.

17 MAG 6961

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information for the GitHub account associated with the user name pedbsktbll, Maintained at Premises Controlled by GitHub, Inc.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: GitHub, Inc.

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by GitHub, Inc. associated with the user name pedbsktbll contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, GitHub, Inc. is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on GitHub, Inc. within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which GitHub, Inc. is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that GitHub, Inc. shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that GitHub, Inc. may disclose this Warrant and Order to an attorney for GitHub, Inc. for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on GitHub, Inc.; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 1:12 A.M.

Date Issued Time Issued

THE HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to GitHub, Inc. (the "Provider") and applies to all content and other information within GitHub, Inc.'s possession, custody, or control that is associated with the user name pedbsktbll (the "Subject Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to GitHub, Inc. GitHub, Inc. is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by GitHub, Inc.

To the extent it is within GitHub, Inc.'s possession, custody, or control, GitHub, Inc. is directed to produce the following information associated with the Subject Account:

a. Use of GitHub Features. All features used by the Subject Account (*e.g.*, code review, project management, integrations, community management, documentation, code hosting, productivity tools). With respect to each feature used by the Subject Account, provide all data posted by or associated with the Subject Account.

b. GitHub Platforms. All platforms used by the Subject Account (*e.g.*, Atom, Electron, GitHub Desktop). With respect to each platform used by the Subject Account, provide all data posted by or associated with the Subject Account.

c. GitHub Repositories. All data from GitHub repositories that were posted by or associated with the Subject Account.

d. Email Content or Direct Message Content. All emails or direct messages sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

e. Address book information. All address book, contact list, or similar information associated with the Subject Account.

f. Subscriber and payment information. All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

g. Transactional records. All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

h. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

i. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by GitHub, Inc. in order to locate any evidence, fruits,

and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses"), including the following:

w. Evidence of the identity(s) of the user(s) of the Subject Account as well as other coconspirators in contact with the Subject Account;

x. Evidence relating to the participation in the Subject Offenses by the users of the Subject Account and others;

y. Evidence concerning financial institutions and transactions used by the users of the Subject Account in furtherance of the Subject Offenses;

z. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

aa. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Account; and

bb. Passwords or other information needed to access any such computers, accounts, or facilities.